ALB:BTK
F.#2016R00227

FILED
IN CLERK'S OFFICE
U.S. DISTRICT COURT E.D.N.Y.
★ NOV 17 2016 ★
LONG ISLAND OFFICE

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF ONE HP PAVILION X360 CONVERTIBLE M3-U103DX LAPTOP COMPUTER, SERIAL NUMBER 8CG637437Q, CURRENTLY IN THE CUSTODY OF THE UNITED STATES PRETRIAL SERVICES AGENCY AT 200 FEDERAL PLAZA, CENTRAL ISLIP, NEW YORK

APPLICATION FOR A SEARCH WARRANT FOR AN ELECTRONIC DEVICE

Case No. MJ - 16 1037

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, DEBRA GERBASI, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I have been employed as a Special Agent with the Department of Homeland Security and its predecessor agencies since 2002, and am currently assigned to the Child Exploitation Group ("CEG"). I have gained expertise in the conduct of child pornography and exploitation investigations through training in seminars, classes, and daily work related

to conducting these types of investigations, including the execution of multiple search warrants relating to child pornography offenses and the subsequent prosecution of offenders.

3. I am familiar with the information contained in this affidavit based on my own personal participation in the investigation, my review of documents, my training and experience, and discussions I have had with other law enforcement personnel concerning the creation, distribution, and proliferation of child pornography. Additionally, statements attributable to individuals herein are set forth in sum and substance and in part.

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

5. The property to be searched is a HP PAVILION X360 CONVERTIBLE M3-U103DX LAPTOP COMPUTER, SERIAL NUMBER 8CG637437Q, hereinafter the "Device." The Device is currently in the custody of the United States Pretrial Services Agency at 200 Federal Plaza, Central Islip, New York.

6. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

PETER LOMBARDI's Child Pornography Possession Conviction

7. On or about November 9, 2016, the United States Pretrial Services Agency seized the Device from PETER LOMBARDI. On June 29, 2016, LOMBARDI pleaded guilty to possessing child pornography in violation of 18 U.S.C. § 2252(a)(4)(B) and (b)(2) before the Honorable Denis R. Hurley. LOMBARDI's conviction arose out of his utilizing an Internet peer-to-peer file-sharing service to download to a computer images and videos of children under the age of eighteen—including some of whom were as young as four—engaging in sex acts.

8. For example, a search of a computer and external hard drive seized from LOMBARDI's Suffolk County, New York residence pursuant to a Search Warrant issued by the Honorable Anne Y. Shields on February 9, 2016 (No. 16-MJ-108) revealed that LOMBARDI downloaded approximately 39,098 images and 2,247 videos of child pornography and child erotica. The majority of the images contained in LOMBARDI's collection consisted of females between the ages of seven to thirteen engaged in sex acts. Many of these images were stamped with the names of websites, such as "LS Models," "LS Island," "Juventa club" and "Ukrainian Angels." In one example of an image stamped "Juventa Club" and seized pursuant to Judge Shield's Search Warrant, an approximately ten-to-twelve year old girl is pictured nude and on her hands and knees.

9. With respect to videos seized pursuant to the Search Warrant, most depicted girls between the ages of eight-to-seventeen, but numerous videos depicted four-to-eight year

old girls. A large number of the videos involved girls in their early teens engaged in sexual activity alone or with another girl in front of a web camera. Many of the videos bore stamps from websites such as "Jailbaitvideos," "candydoll.tv," "Fallen Angels," and "Galitisin-news.com." For example, in a video stamped with the name of the "Galitsin-news.com" website, two girls between the ages of twelve and fifteen climb across a dining table and engage in sexual activity, fondling one another, digitally penetrating each other and performing oral sex on each other.

10. Following his arrest on February 11, 2016, LOMBARDI waived his Miranda rights and spoke to me and other law enforcement officers about his possession of child pornography. In sum and substance, LOMBARDI stated that he understood that child pornography constituted images of children under the age of eighteen involved in sex acts. LOMBARDI further stated that he used search terms such as "PTHC" ("Preteen Hardcore") to search for images and videos of child pornography on the Bit Torrent peer-to-peer file sharing service. LOMBARDI also stated that he would save images of child pornography to his external hard drive or to folders on his laptop computer. LOMBARDI further stated that his main interest was in images of child pornography involving sixteen-to-eighteen year old girls.

The Defendant's Bail Conditions

11. Following his arrest on February 11, 2016, LOMBARDI was released on bond with a variety of conditions. As relevant here, LOMBARDI was prohibited from using a computer or the Internet for any purposes other than those related to his employment,

communication with Pretrial Services, his counsel or mental health treatment provider or for purposes approved in advance by Pretrial Services. Under another condition of his release, LOMBARDI agreed to allow Pretrial Services to use software to monitor his use of his computer and the Internet.

12. Initially, LOMBARDI elected not to use a computer. However, on October 24, 2016, he informed Pretrial Services that he wanted to utilize a laptop, which is described in this Affidavit as "the Device." Consequently, Pretrial Services installed monitoring software on the Device. The monitoring software showed that between October 31, 2016 and November 2, 2016, LOMBARDI used the Device to search the Internet for material that depicted teenagers engaged in sexual activity.

13. For example, on October 30, 2016, the monitoring software detected that LOMBARDI used the Device to search eBay.com for "russian teens." Running that search results in being directed to a page containing a variety of hyperlinks, including a hyperlink to the website "wow.com," an internet search engine that contains other hyperlinks, including "Russian Teens – Teen Sex Galleries." Following one of the wow.com hyperlinks leads to the website containing additional hyperlinks to websites, including "http://daughters.lolataboo.com/." Clicking on that hyperlink leads to images containing adult males engaged in sexually activity with prepubescent girls, whom based upon my training and experience appear younger eighteen. In addition, the monitoring software showed that one of LOMBARDI's eBay searches led to a photograph of teenage girls

engaged in sexual activities that was captioned "Teen Erotica" and "Teenage Sex Addicts 4."[1]

14. I am further informed by Pretrial Services staff that the monitoring software used on the device would not enable Pretrial Services to conduct a full forensic search of the Device, such as that sought through this Affidavit. Moreover, in light of LOMBARDI's previous downloads of child pornography and his admitted interested in child pornography involving teenage girls under the age of eighteen, the monitored activity on the Device demonstrates that there is probable cause to believe that a full forensic search of the Device will result in the seizure of additional child pornography.

15. The Device is currently in the lawful possession of Pretrial Services. It came into Pretrial Services's possession in the following way: the Device was seized after Pretrial Service's monitoring software detected that LOMBARDI had used the Device in violation his bail conditions. Therefore, while Pretrial Services might already have all necessary authority to examine the Device, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Device will comply with the Fourth Amendment and other applicable laws.

16. The Device is currently in storage at Pretrial Services's Office located at 200 Federal Plaza, Central Islip, New York. In my training and experience and based upon my discussions with Pretrial Services staff, who were assigned to supervising LOMBARDI's

---

[1] Photocopies of the images referred to in paragraph 13 are available for the Court's review.

release,[2] I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of Pretrial Services.

TECHNICAL TERMS

17. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

---

[2] On November 9, 2016, the Honorable Steven I. Locke revoked LOMBARDI's bail and entered an Order of Permanent Detention pending LOMBARDI's January 27, 2016 sentencing. That same day, the Honorable Joan M. Azrack affirmed Judge Locke's Order of Permanent Detention.

c. A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

18. Based on my training, experience, and research, I know that the Device has capabilities that allow it to: access and download information from the Internet; send, receive, and store e-mail; store and play back audio files; store dates, appointments, and other information; take, send, receive, and store still photographs and moving video; and to function as a tablet. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the Device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

19. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been

viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

20. There is probable cause to believe that things that were once stored on the Device may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it.

To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

21. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

22. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

23. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

24. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

Debra Gerbasi

Debra Gerbasi
Special Agent
Department of Homeland Security

Subscribed and sworn to before me
on November 17, 2016:

/s/ Steven I. Locke
THE HONORABLE STEVEN I. LOCKE
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

The property to be searched is a HP PAVILION X360 CONVERTIBLE M3-U103DX LAPTOP COMPUTER, SERIAL NUMBER 8CG637437Q, hereinafter the "Device." The Device is currently in the custody of the United States Pretrial Services Agency at 200 Federal Plaza, Central Islip, New York.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of Title 18, United States Code Sections 2252 and 2252A and involve PETER LOMBARDI since February 11, 2016, including:

a. Images of child pornography and files containing images of child pornography and records, images, information or correspondence pertaining to the possession, access with intent to view, receipt and distribution of sexually explicit material relating to children, in violation of Title 18, United States Code, Sections 2252 and 2252A, in any form wherever they may be stored or found;

b. Originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

c. Motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

d. Records, information or correspondence pertaining to the possession, access with intent to view, transportation, receipt, distribution and reproduction of sexually explicit material relating to children, as defined in 18 U.S.C. § 2256, including, but not limited to:

i. correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

e. Billing and payment records, including records from credit card companies, PayPal and other electronic payment services, reflecting access to websites pertaining to child pornography;

f. Records or other items which evidence ownership or use of computer related equipment, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes;

g. Address books, mailing lists, supplier lists, mailing address labels and any and all documents and records pertaining to the preparation, purchase and acquisition of names or lists of names to be used in connection with the purchase, sale, trade or transmission of any visual depiction of minors engaged in sexually explicit conduct;

h. Address books, names, lists of names and addresses of individuals believed to be minors;

i. Materials and photographs depicting sexual conduct between adults and minors or used in sexual conduct between adults and minors;

j. Any and all records, documents, invoices and materials that concern any Internet accounts used to possess, receive or distribute child pornography; and

k. Computer-related documentation, meaning any written, recorded, printed, or electronically stored material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

2. Evidence of who used, owned, or controlled the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence. User attribution information (i.e. files and other data such as chats or e-mails) relevant to the trading of child pornography. Such information tends to show the identity of the person using the computer near the time of the criminal activity;

3. Evidence of software that would allow others to control the computer, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

4. Evidence of the lack of such malicious software;

5. Evidence of the attachment to the computer of other storage devices or similar containers for electronic evidence;

6. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the computer;

7. Evidence of the times the computer was used;

8. Passwords, encryption keys, and other access devices that may be necessary to access the computer;

9. Documentation and manuals that may be necessary to access the computer or to conduct a forensic examination of the computer;

10. Evidence of Peer to Peer software;

11. contextual information necessary to understand the evidence described in this attachment.

If any materials protected by the Privacy Protection Act, 42 U.S.C. § 2000aa are inadvertently seized, all efforts will be made to return these materials to their authors as quickly as possible.

12. Records of Internet Protocol addresses used;

13. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

all of which constitute evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252 and 2252A.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

Definitions

a. "Child Erotica," as used herein, means materials and items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene and that do not necessarily depict minors in sexually explicit poses or positions.

b. "Child Pornography," as used herein, includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct), as well as any visual depiction, the production of which involves the use of a minor engaged in sexually explicit conduct (see 18 U.S.C. §§ 2252 and 2256(2)).

c. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

d. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital, oral genital, or oral anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. See 18 U.S.C. § 2256(2).

e. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device[.]"

f. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); and peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

g. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

h. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

i. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. "Domain name" is a name that identifies an IP address.

j. "Peer to Peer" (also known as "P2P") is a file sharing program that allows people to exchange documents and files between computers. Many of the software programs are available for free on the Internet. When installed, the P2P program allows the installer to designate certain files to share, generally placed in a "shared folder." The files located in the "shared folder" are accessible to anyone who uses the same program by simply searching for specific files and downloading the files. As further detailed below, with regard to the proliferation of child pornography, P2P software, such as "Limewire," "Bearshare," and "Frostwire" are often used to exchange images of child pornography.

k. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).